UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,632	04/06/2001	Aki Yokote	10745/6	1014

757 7590 08/26/2004

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
MAURO JR, THOMAS J	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 08/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/827,632	YOKOTE, AKI	
	Examiner	Art Unit	
	Thomas J. Mauro Jr.	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/6/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending and are presented for examination. A formal action on the merits of claims 1-21 follows.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. The term "long" in claim 8 is a relative term which renders the claim indefinite. The term "long" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably appraised of the scope of the invention. Therefore for the purposes of examination, because long is indefinite, Examiner will provide his/her own meaning of the word in the claim interpretation.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-2 are rejected under 35 U.S.C. 102(e) as being anticipated by Igarashi et al. (US 2001/0012777).

With respect to claim 1, Igarashi teaches the invention substantially as claimed, a method of implementing Internet protocol security in a mobile IP network, comprising the steps of:

initiating communication from a first node to a second node **[Igarashi -- Page 5 paragraph [0088] – The correspondent node (CN) initiates communication in order to communicate with the mobile node (MN)]**; and

checking by the first node if any security association is established with the second node **[Igarashi -- Page 3 paragraph [0045], page 4 paragraph [0075] and pages 5-6 paragraphs [0106, 0110 and 0113] – A bindings cache stores binding information used for communication between the nodes. Thus it is obvious that it is stored to be used again when communicating with the mobile node and therefore is checked before registering any additional security associations]**; and

initiating by the first node establishment of a security association for protecting communications with the second node **[Igarashi -- Page 5 paragraph [0088 – CN contacts authentication server to receive required parameters, i.e. security associations, for communicating securely with the MN]**.

With respect to claim 2, Igarashi further teaches wherein the second node is a mobile node situated away from its home link **[Igarashi -- Page 4 paragraph [0069] – MN, i.e. mobile node, moves to sub network away from home agent, i.e. home link, to a foreign agent]**.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777).

Regarding claim 3, Igarashi teaches wherein the first node initiates communication with the second node by sending a control packet to the second node through the second node's home agent and the second node in response returns a binding updates to the first node **[Igarashi -- Page 4 paragraphs [0069 and 0072-0073] – After initiating communication, Home agent (HA) issues to the CN an instruction to update the network binding information for communicating with the MN]**.

Igarashi fails to explicitly teach using a control packet to initiate communication.

The use of control packets for communicating between nodes is notoriously well known in the art and is used to begin communication with nodes before actual data, i.e. secured data, is sent. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention for the initiating packet to be a control packet in order to provide for the establishment of communication and binding updates before sending data in order to prevent any misuse of or integrity loss in data.

9. Claims 4-5 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777), as applied to claim 1 and 4 above respectively, in view of Swander (US 2004/0049585).

Regarding claim 4, Igarashi teaches the invention substantially as claimed, as aforementioned in claim 1 above, but fails to explicitly teach wherein the security association (SA) employs a Kerberos key exchange.

Swander, however, discloses a system for initiating communication between a CN and a MN in which the CN initiates and proposes security associations (SA) to the MN, upon which, the SA is a Kerberos key **[Swander -- Page 3 paragraph [0028]]**.

Both Igarashi and Swander are concerned with securely transmitting data between a CN and an MN in a mobile IP network.

The use of Kerberos keys were notoriously well known and widely for encrypting data sent between two nodes.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the use of a Kerberos key, as taught by Swander into the invention of Igarashi, in order securely encrypt data between nodes using a very secure and widely known and used encrypting technique.

Regarding claim 5, Igarashi-Swander teach the invention substantially as claimed, as aforementioned in claim 4 above, including wherein one of the first and second nodes uses a secret key established in layer 2 for layer 3 authentication **[Igarashi -- Page 5 paragraph [0088] – CN obtains authentication information, i.e. key establishment, at the link layer, i.e. layer 2. This will then be used by the next layer, i.e. layer 3, to provide authentication]**.

Regarding claim 8, Igarashi-Swander teach the invention substantially as claimed, including wherein the SA has a long lifetime and is used over multiple sessions of communications between the nodes **[Swander -- Page 3 paragraphs 0025-0026] – SA's are continued to be used until the association expires, thereby giving them a long lifetime, i.e. more than one session]**.

10. Claims 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777), as applied to claim 1 above, in view of Leung (U.S. 6,760,444).

Regarding claim 6, Igarashi teaches the invention substantially as claimed, as aforementioned in claim 1 above, but fails to explicitly teach wherein the network has security association managers, and the security association is established by the security association managers.

Leung, however, discloses a mobile IP authentication system which employs the use of a server, i.e. SA manager, for storing and obtaining security associations in a table **[Leung -- Col. 8 lines 51-67 – Col. 9 lines 1-15]**.

Both Igarashi and Leung are concerned with providing authentication security in a mobile IP network.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of a security association manager, i.e. server, as taught by Leung into the invention of Igarashi, in order to minimize administrative support and to relieve the burden of the minimal resource mobile node devices with less memory **[Leung -- Col. 9 lines 7-15]**.

Regarding claim 16, Leung teaches an IP network comprising:

nodes communicating with each other over the network **[Igarashi -- Page 5 paragraph [0088] – CN communicate over a mobile network with an MN]**; and

establishing a security association for distribution to a first node, if no security association currently exists **[Igarashi -- Page 5 paragraph [0088 – CN contacts authentication server to receive required parameters, i.e. security associations, for communicating securely with the MN]**.

Igarashi fails to explicitly teach a security association manager for managing and storing security associations associated with network nodes.

Leung, however, discloses a mobile IP authentication system which employs the use of a server, i.e. SA manager, for storing and obtaining security associations in a table **[Leung -- Col. 8 lines 51-67 – Col. 9 lines 1-15]**.

Both Igarashi and Leung are concerned with providing authentication security in a mobile IP network.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of a security association manager, i.e. server, as taught by Leung into the invention of Igarashi, in order to minimize administrative support and to relieve the burden of the minimal resource mobile node devices with less memory **[Leung -- Col. 9 lines 7-15]**.

11. Claims 7 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777), as applied to claim 1 above, in view of Johnston (U.S. 6,373,946).

Regarding claim 7, Igarashi teaches the invention substantially as claimed, as aforementioned in claim 1 above, but fails to explicitly teach wherein the first and second nodes have a subscriber identification module (SIM), for storing the SA's.

Johnston, however, discloses a GSM system for implementing security between mobile nodes in a telecommunications environment which employs the use of a SIM which stores and provides a key for deciphering **[Johnston -- Col. 2 lines 66-67 – Col. 3 lines 1-13 and Col. 9 lines 14-21]**. Both Igarashi and Johnston are concerned with providing communications security using keys for mobile users.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of a SIM module for storing security keys, as taught by Johnston into the invention of Igarashi, in order to provide a secure way of storing the key such that it cannot be ready or deciphered illegally **[Johnston -- Col. 1 lines 23-37]**.

Regarding claim 11, Igarashi-Johnston teach the invention substantially as claimed, including wherein the network complies with International Mobile Telecommunications-2000 standards **[Johnston -- Col. 1 line 13-37 – GSM networks comply with IMT-2000]**.

12. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777), as applied to claims 1 and 9 above respectively, in view of Ala-Laurila et al. (U.S. 6,587,680).

Regarding claims 9-10, Igarashi teaches the invention substantially as claimed, as aforementioned in claim 1 above, but fails to explicitly teach wherein communication is a real-

time interactive digital data communication (claim 9), more specifically, voice over internet protocol (VOIP) (claim 10).

Ala-Laurila, however, discloses a system for transferring security association between terminals during a handover which is made very fast by minimizing traffic in order to prevent any interruption of real-time services, such as voice over IP and video distribution **[Ala-Laurila -- Col. 8 lines 1-16]**.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the real-time data services such as Voice over IP, as taught by Ala-Laurila into the invention of Igarashi, in order to extend the requirements of fast connection and negotiation between nodes as required by real-time data services.

13. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777) in view of Faccin et al. (US 2002/0120844).

Regarding claim 12, Igarashi teaches a method for implementing security in a mobile IP network, comprising the steps of:

establishing a layer 2 secret key between a node and a base station when the node is establishing wireless connection with the station **[Igarashi -- Page 5 paragraph [0088] – Node establishes a link layer, i.e. layer 2, key, i.e. authentication parameter, for communication with a node]**;

reporting the established layer 2 secret key from a layer 2 to a layer 3 in the node **[Igarashi -- Page 5 paragraph [0088] – CN obtains authentication information, i.e. key establishment, at the link layer, i.e. layer 2. It is obvious that this key will then be used by the next layer, i.e. layer 3, to actually provide the authentication by use of the key already established in layer 2]**; and

using the reported layer 2 secret key to authenticate the node **[Igarashi -- Page 5 paragraph [0088] – Once parameters are received at proxy CN and are authorized for communication, communication proceeds to authenticate the node]**.

Igarashi fails to teach using the key for authentication upon logging into a network

Faccin, however, discloses an authentication and distribution of keys in a mobile IP network in which a mobile node is authenticated in a network when the node is powered on or when it visits, i.e. logs into, another network **[Faccin -- Page 2 paragraphs [0024-0030]]**.

It would have been obvious to a person of ordinary skill in the art a the time the invention was made to incorporate the authentication to the network upon logging in, as taught by Faccin into the invention of Igarashi, in order to optimize the authentication process by providing mutual, i.e. both node and network, authentication together.

14. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777) and Faccin et al. (US 2002/0120844), as applied to claims 12 and 13 above respectively, in view of Ala-Laurila et al. (U.S. 6,587,680).

Regarding claim 13-14, these are method claims similar to the method claimed in claims 9-10 above. They contain similar limitations; therefore, claims 13-14 are rejected under the same rationale.

15. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777) and Faccin et al. (US 2002/0120844), as applied to claim 12 above, in view of Johnston (U.S. 6,373,946).

Regarding claim 15, this is a method claim similar to the method claimed in claim 11 above. It has similar limitations; therefore claim 15 is rejected under the same rationale.

16. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777) and Leung (U.S. 6,760,444), as applied to claims 16 and 17 above respectively, in view of Swander (US 2004/0049585).

Regarding claim 17, Igarashi-Leung teach the invention substantially as claimed, as aforementioned in claim 16 above, but fails to teach using a Kerberos key exchange along with a key distribution center for distributing session keys.

Swander, however, discloses a system for initiating communication between a CN and a MN in which the CN initiates and proposes security associations (SA) to the MN, upon which, the SA is a Kerberos key **[Swander -- Page 3 paragraph [0028]]**.

Both Igarashi and Swander are concerned with securely transmitting data between a CN and an MN in a mobile IP network.

The use of Kerberos keys were notoriously well known and widely for encrypting data sent between two nodes which obviously requires the use of a key distribution center (KDC) for distributing the Kerberos session keys.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the use of a Kerberos key and accompanying KDC, as taught by Swander into the invention of Igarashi, in order securely encrypt data between nodes using a very secure and widely known and used encrypting technique.

Regarding claim 18, Igarashi-Leung-Swander teach the invention substantially as claimed, as aforementioned in claim 17 above, including wherein the security association manager requests the KDC to issue a session key **[Igarashi -- Page 5 paragraph [0088] – When CN wishes to communicate with MN, request is made to authentication server for the necessary parameters, i.e. Kerberos keys (Swander Page 3 paragraph [0028]), which are then obviously requested from a KDC]**.

17. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777) and Leung (U.S. 6,760,444), as applied to claims 16 and 19 above respectively, in view of Ala-Laurila et al. (U.S. 6,587,680).

Regarding claims 19-20, these are method claims similar to the method claimed in claims 9-10 above. They have similar limitations; therefore, claims 19-20 are rejected under the same rationale.

18. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Igarashi et al. (US 2001/0012777) and Leung (U.S. 6,760,444), as applied to claim 16 above, in view of Johnston (U.S. 6,373,946).

Regarding claim 21, this is a method claim similar to the method claimed in claim 11 above. It has similar limitations; therefore, claim 21 is rejected under the same rationale.

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Forslow (US 2002/0133534) discloses the formation of an extranet workgroup between two MN's requiring authentication to be established.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas J. Mauro Jr. whose telephone number is 703-605-1234. The examiner can normally be reached on M-F 8:00a.m. - 4:30p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on 703-308-5221. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TJM
August 16, 2004

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100